Über einige merkwürdige Polynome in endlichen Körpern mit zahlentheoretischen Beziehungen.

Von LADISLAUS RÉDEI in Szeged.

Herrn Prof. Michael Bauer, meinem verehrten Lehrer, zum 70. Geburtsjahre gewidmet.

Gegeben sei ein endlicher Primkörper P von der Charakteristik p ($\geqq 3$) und eine natürliche Zahl n. Wir werden gewisse Polynome (einer Variablen) in P untersuchen. Dabei ziehen wir manchmal auch den (endlichen) Erweiterungskörper Q mit der Elementenzahl

$$q = p^n \tag{1}$$

in Betracht. (Für $n = 1$ ist $Q = P$.) Alle unsere Feststellungen über P lassen sich natürlich in die Kongruenzsprache umsetzen und erhalten dadurch einen einfachen zahlentheoretischen Sinn. Hierüber werden wir näheres bemerken dort, wo das für nötig erscheint. Den Körper der absolut rationalen Zahlen bezeichnen wir mit R. Wie das üblich ist, sollen die Symbole $0, 1, \ldots, p-1$, also allgemeiner die für p ganzen, rationalen Zahlen, auch die Elemente von P bezeichnen. Hiedurch könnte ein Mißverständnis entstehen, wir verabreden uns aber, daß „rationale Zahlen" (insbesondere Polynome und Potenzreihen mit solchen Koeffizienten) in P zu deuten sind, und nur dann in R, wenn es ausdrücklich gesagt oder augenscheinlich wird.

Wir wollen auf die bekannte Tatsache hinweisen, daß in Q keine weiteren Funktionen als die Polynome existieren, und zwar ist das durch die Interpolationsformel

$$\sum_{a \text{ in } Q} a' [1-(x-a)^{q-1}] \tag{2}$$

gelieferte Polynom das einzige vom Grade $< q$, das die allgemeinste eindeutige Funktion $a \to a'$ von einer Variablen in Q realisiert. [In Q sind „alle Polynome" (von beliebigem Grad) ein durchaus umfassenderer Begriff als „alle Funktionen".]. Kein Wunder, daß in den endlichen Körpern den Polynomen ein hohes Interesse zukommt.

Die Theorie der Polynome in Q ist in mehrerer Hinsicht vielgestalteter und schwieriger als in R oder im Körper der komplexen

Zahlen. (Das ist wohl dem Umstand zuzuschreiben, daß man in Q über Teilbarkeit, Anordnung und Bewertung nicht sprechen kann.) So ist unter anderem eine Besonderheit in Q, daß ein Polynom kein Quadrat zu sein braucht, wenn sein Wertevorrat aus lauter Quadratelementen besteht[1]). Vielmehr gibt es nach (2) offenbar $\left(\frac{q+1}{2}\right)^q$ Polynome der letzteren Art und vom Grade $< q$, darunter aber nur $\frac{1}{2}(q^{\frac{q+1}{2}}+1)$ also für großes q wesentlich weniger Quadratpolynome. Z. B. nehmen die Polynome

$$1+x^2+2x^{\frac{q+1}{2}}, \quad 2x^2(1+x^{\frac{q-1}{2}})$$

nur Quadratelemente an, ohne selbst Quadratpolynome zu sein.

Nunmehr setzen wir in P

$$\Phi_{++}(x) = \frac{1}{2}\,[1+x^{\frac{q+1}{2}}+(1-x)^{\frac{q+1}{2}}], \tag{3}$$

$$\Phi_{+-}(x) = \frac{2}{x}\,[1+x^{\frac{q+1}{2}}-(1-x)^{\frac{q+1}{2}}], \tag{4}$$

$$\Phi_{-+}(x) = \frac{1}{2(1-x)}[1-x^{\frac{q+1}{2}}+(1-x)^{\frac{q+1}{2}}], \tag{5}$$

$$\Phi_{--}(x) = \frac{2}{x(1-x)}[1-x^{\frac{q+1}{2}}-(1-x)^{\frac{q+1}{2}}]. \tag{6}$$

Man sieht gleich, daß diese (ganzen) Polynome normiert sind, d. h. ihr konstantes Glied 1 ist[2]). Übrigens lassen sie sich in einer Formel so angeben:

$$\Phi_{\varrho\sigma}(x) = 2^{-\sigma}x^{\frac{\sigma-1}{2}}(1-x)^{\frac{\varrho-1}{2}}[1+\varrho x^{\frac{q+1}{2}}+\sigma(1-x)^{\frac{q+1}{2}}] \quad (\varrho,\sigma=\pm 1).^3) \tag{7}$$

[1]) Besteht aber der Wertevorrat eines Polynoms $f(x)$ in R aus lauter Quadratelementen, so ist es ein Quadratpolynom in R, da nämlich der Annahme nach das Polynom $y^2-f(x)$ von x, y für jedes x in R reduzibel ist, und so ist es nach HILBERT selbst reduzibel.

[2]) Die Polynome (3)—(6) lassen sich mit folgender einfacher Vorschrift definieren. Man gehe aus dem einzigen Polynom $(1-x)^{\frac{q+1}{2}}$ aus, streiche oder verdoppele die äußeren Glieder 1, $\pm x^{\frac{q+1}{2}}$ voneinander unabhängig, streiche in den erhaltenen vier Polynomen die etwaigen Faktoren x, $1-x$, und normiere sie. So entstehen (3)—(6). — Aus inneren Gründen wäre richtiger gewesen, die Reihenfolge der rechten Seiten in (3)—(6) umzukehren und ebenso später unten in (8)—(11). Das hätte nämlich insbesondere zur Folgerung, daß in (30) sich ϱ, σ für $-\varrho, -\sigma$ schreiben ließe. Obigen Bezeichnungen haben wir aus formalen Gründen den Vorzug gegeben.

[3]) Statt der Indizes ϱ, σ geben wir oft nur das Vorzeichen an, wie auch schon in (3)—(6).

Andererseits betrachten wir die folgenden größten gemeinschaftlichen Teiler in P:

$$(8) \qquad \varphi_{++}(x) = (1+x^{\frac{q-1}{2}},\ 1+(1-x)^{\frac{q-1}{2}}),$$

$$(9) \qquad \varphi_{+-}(x) = (1+x^{\frac{q-1}{2}},\ 1-(1-x)^{\frac{q-1}{2}}),$$

$$(10) \qquad \varphi_{-+}(x) = (1-x^{\frac{q-1}{2}},\ 1+(1-x)^{\frac{q-1}{2}}),$$

$$(11) \qquad \varphi_{--}(x) = (1-x^{\frac{q-1}{2}},\ 1-(1-x)^{\frac{q-1}{2}}),$$

die wir ebenfalls gleich als normierte Polynome annehmen, wodurch sie eindeutig bestimmt sind[4]). In einer Formel vereinigt:

$$(12) \qquad \varphi_{\varrho\sigma}(x) = (1+\varrho x^{\frac{q-1}{2}},\ 1+\sigma(1-x)^{\frac{q-1}{2}}).$$

In den folgenden werden wir uns hauptsächlich mit diesen Polynomquadrupeln (3)—(6), (8)—(11) beschäftigen. Unser bemerkenswertestes Resultat ist die Bestimmung der größten gemeinschaftlichen Teiler (8)—(11) [Sätze 4, 8] und hiedurch zugleich die Faktorenzerlegungen in Satz 5. Auf eine nähere Beschreibung des Inhalts dieser Arbeit verzichten wir hier, verweisen aber hierfür auf die an die Sätze gefügten Fußbemerkungen und auf die Bemerkung am Schluß der Arbeit.

Satz 1. *Der Wertevorrat von $\Phi_{\varrho\sigma}(x)$ in Q besteht aus lauter Quadratelementen. Und zwar ist $\Phi_{\varrho\sigma}(0)=1$, $\Phi_{\varrho\sigma}(1)=2^{\varrho-\sigma}$, und für ein $x\neq 0, 1$ ist der Wert von $\Phi_{\varrho\sigma}(x)$ aus folgender Tabelle zu entnehmen, wobei $\chi(x)$ den quadratischen Charakter in Q bezeichnet.*[5])

(13)

$\chi(x)$	+	+	−	−
$\chi(1-x)$	+	−	+	−
$\Phi_{++}(x)$	1	x	$1-x$	0
$\Phi_{+-}(x)$	4	$\frac{4}{x}$	0	$\frac{4(1-x)}{x}$
$\Phi_{-+}(x)$	1	0	$\frac{1}{1-x}$	$\frac{x}{1-x}$
$\Phi_{--}(x)$	0	$\frac{4}{x}$	$\frac{4}{1-x}$	$\frac{4}{x(1-x)}$

[4]) Diese Polynome (8)—(11) habe ich für $q=p$ auch schon in einer früheren (ungarischen) Arbeit „Eine Anwendung der hypergeometrischen Reihen auf eine Faktorenzerlegung des Fermatschen Polynoms $1-x^{p-1}$ im Zusammenhang mit der Theorie der quadratischen Reste, *Math. u. Naturwiss. Anzeiger d. ung. Akad.* (im Erscheinen)" untersucht und für sie einige der hiesigen Resultate festgestellt. — Legte man R statt P zu Grunde, so wäre $\varphi_{\varrho\sigma}(x)$ leicht angebbar, und zwar gleich 1 oder $1-x+x^2$.

[5]) D. h. $\chi(0)=0$ und $\chi(x)=1$ oder -1 $(x\neq 0)$, je nachdem x ein Quadratelement ist oder nicht. Im Fall $q=p$ ist $\chi(x)$ im wesentlichen das Symbol $\left(\frac{x}{p}\right)$ von LEGENDRE. — In obiger Tabelle geben wir von $\chi(x)$ und $\chi(1-x)$ nur das Vorzeichen an.

Satz 2. *Die $\Phi_{\varrho\sigma}(x)$ sind Polynomquadrate in P und zwar ist*

$$\Phi_{\varrho\sigma}(x) = \varphi^2_{\varrho\sigma}(x) \qquad (\varrho, \sigma = \pm 1).^{6}) \tag{14}$$

Satz 3. *Bezeichne $n_{\varrho\sigma}$ den Grad von $\varphi_{\varrho\sigma}(x)$. Es ist*

$$n_{++} = \frac{q-\varepsilon}{4},\ n_{+-} = n_{-+} = \frac{q-\varepsilon}{4} - \frac{1-\varepsilon}{2},\ n_{--} = \frac{q-\varepsilon}{4} - 1, \tag{15}$$

oder in einer Formel

$$n_{\varrho\sigma} = \frac{1}{4}(q - 2 + \varrho + \sigma - \varepsilon\varrho\sigma), \tag{15'}$$

wobei

$$\varepsilon = \chi(-1) = (-1)^{\frac{q-1}{2}}.^{7}) \tag{16}$$

Zum folgenden nehmen wir die hypergeometrische Reihe

$$F(\alpha, \beta, \gamma, x) = 1 + \frac{\alpha \cdot \beta}{\gamma \cdot 1} x + \frac{\alpha(\alpha+1) \cdot \beta(\beta+1)}{\gamma(\gamma+1) \cdot 2!} x^2 + \dots$$

zu Hilfe. Wie es schon GAUSS[8]) bemerkt hat, ist insbesondere

$$F\left(\frac{1}{2} - \frac{\nu}{2}, -\frac{\nu}{2}, \frac{1}{2}, x\right) = \tag{17}$$

$$= \frac{1}{2}[(1+\sqrt{x})^\nu + (1-\sqrt{x})^\nu] = 1 + \sum \binom{\nu}{2k} x^k,$$

$$F\left(\frac{1}{2} - \frac{\nu}{2}, 1 - \frac{\nu}{2}, \frac{3}{2}, x\right) = \tag{18}$$

$$= \frac{1}{2\nu\sqrt{x}}[(1+\sqrt{x})^\nu - (1-\sqrt{x})^\nu] = 1 + \frac{1}{\nu}\sum \binom{\nu}{2k+1} x^k,$$

wobei für $k = 1, 2, \dots$ zu summieren ist. Man setze zuerst $\nu = \frac{1}{2}$, dann $\nu = -\frac{1}{2}$, und bezeichne die entstandenen Funktionen so:

$$F_{++}(x) = F\left(\frac{1}{4}, -\frac{1}{4}, \frac{1}{2}, x\right) = \frac{1}{2}[(1+\sqrt{x})^{\frac{1}{2}} + (1-\sqrt{x})^{\frac{1}{2}}], \tag{19}$$

$$F_{+-}(x) = F\left(\frac{1}{4}, \frac{3}{4}, \frac{3}{2}, x\right) = \frac{1}{\sqrt{x}}[(1+\sqrt{x})^{\frac{1}{2}} - (1-\sqrt{x})^{\frac{1}{2}}], \tag{20}$$

---

[6]) Alles was wir im folgenden über $\varphi_{\varrho\sigma}(x)$ aussagen, ist kraft (14) auch für $\Phi_{\varrho\sigma}(x)$ verwertbar.

[7]) Also ist $\varepsilon = 1$ oder -1, je nachdem $q \equiv 1$ oder $-1 \pmod 4$ ist.

[8]) GAUSS, Werke, 3 (1870), S. 127. Vgl. auch H. A. SCHWARZ, Über diejenigen Fälle, in welchen die Gaußische hypergeometrische Reihe eine algebraische Funktion ihres vierten Elementes darstellt, *Journ. f. Math.*, **75** (1873), S. 292–335. Übrigens lassen sich (17) und (18) leicht unmittelbar verifizieren.

$$(21)\quad F_{-+}(x)=F\left(\frac{3}{4},\frac{1}{4},\frac{1}{2},x\right)=\frac{1}{2}[(1+\sqrt{x})^{-\frac{1}{2}}+(1-\sqrt{x})^{-\frac{1}{2}}],$$

$$(22)\quad F_{--}(x)=F\left(\frac{3}{4},\frac{5}{4},\frac{3}{2},x\right)=-\frac{1}{\sqrt{x}}[(1+\sqrt{x})^{-\frac{1}{2}}-(1-\sqrt{x})^{-\frac{1}{2}}].$$

Wieder in einer Formel vereinigt:

$$(23)\quad F_{\varrho\sigma}(x)=2^{-\frac{1+\sigma}{2}}(\sqrt{x})^{\frac{\sigma-1}{2}}(\sqrt{1-x})^{\frac{\varrho-1}{2}}[(1+\sqrt{x})^{\frac{1}{2}}+\sigma(1-\sqrt{x})^{\frac{1}{2}}].$$

Man rechnet leicht nach, daß folgende Reihenentwicklungen gelten:

$$(24)\quad F_{++}(x)=1+\sum\binom{\frac{1}{2}}{2k}x^k=1-\sum\frac{4(4k-3)!}{(2k-2)!\,(2k)!}\left(\frac{x}{16}\right)^k,$$

$$(25)\quad F_{+-}(x)=1+2\sum\binom{\frac{1}{2}}{2k+1}x^k=1+\sum\frac{2(4k-1)!}{(2k-1)!\,(2k+1)!}\left(\frac{x}{16}\right)^k,$$

$$(26)\quad F_{-+}(x)=1+\sum\binom{-\frac{1}{2}}{2k}x^k=1+\sum\frac{2(4k-1)!}{(2k-1)!\,(2k)!}\left(\frac{x}{16}\right)^k,$$

$$(27)\quad F_{--}(x)=1-2\sum\binom{-\frac{1}{2}}{2k+1}x^k=1+\sum\frac{(4k+1)!}{(2k)!\,(2k+1)!}\left(\frac{x}{16}\right)^k.$$

Satz 4. *Es ist $\varphi_{\varrho\sigma}(x)$ eine Partialsumme von $F_{\varrho\sigma}(x)$ $[\varrho,\sigma=\pm 1]$.*[9]

Satz 5. *In P gelten die Faktorenzerlegungen*

$$(28)\quad 1+x^{\frac{q-1}{2}}=\varphi_{++}(x)\,\varphi_{+-}(x),\quad 1-x^{\frac{q-1}{2}}=(1-x)\,\varphi_{-+}(x)\,\varphi_{--}(x),$$

zugleich also auch

$$(29)\quad 1-x^{q-1}=(1-x)\,\varphi_{++}(x)\,\varphi_{+-}(x)\,\varphi_{-+}(x)\,\varphi_{--}(x).$$[10]

---

[9]) Satz 4 mit (15) zusammen bestimmt die Polynome $\varphi_{\varrho\sigma}(x)$ auf Grund der Reihenentwicklungen (24)—(27) vollkommen mit explizit angegebenen Koeffizienten (diese sind natürlich in P aufzufassen). [Vgl. hierzu [13]).] Hierdurch wurde mit Vorwegnahme der Sätze 5 und 6 viererlei geleistet, und zwar wurde nach (14) die Quadratwurzel aus den Polynomen (3)—(6) ausgezogen, die größten gemeinschaftlichen Teiler (8)—(11), also auch die elementarsymmetrischen Funktionen der Elemente a in (30) bestimmt, und die (effektiven) Faktorenzerlegungen (28), (29) bewirkt. Man kann sagen, daß es sich in allem diesem um eine Eigenschaft der Potenzreihen (24)—(27) handelt. Dabei ist am auffälligsten, das besonders betont werden soll, daß die zu allen Paaren p, n gehörenden zweimal unendlich vielen Polynomquadrupel (8)—(11) [die ja obendrein in den verschiedenen Primkörpern P erklärt sind] aus einer gemeinsamen Quelle entstehen, nämlich (kurz gesagt) als Partialsummen von vier festen Potenzreihen.

[10]) Uns waren bisher nur die folgenden Faktorenzerlegungen des „Fermatschen" Polynoms $1-x^{q-1}$ bekannt:

$$\prod_{a\,(\neq 0)\text{ in }Q}(1-ax)\quad(1-x^m)(1+x^m+x^{2m}+\ldots+x^{q-1-m})\quad[m\,|\,q-1].$$

Hieraus folgt, daß die $\varphi_{\varrho\sigma}(x)$ in Q in lauter verschiedene lineare Faktoren zerfallen.

Satz 6. *Die Nullstellen von $\varphi_{\varrho\sigma}(x)$ sind die Elemente a in Q mit*

$$\chi(a) = -\varrho,\ \chi(1-a) = -\sigma.^{11}) \tag{30}$$

Satz 7. *Das Verhalten von $\varphi_{\varrho\sigma}(x)$ bei Ausübung der Elemente der anharmonischen Gruppe auf x ist durch die Formeln*

$$\varphi_{++}(1-x) = \chi(2)\varphi_{++}(x),\quad x^{n++}\varphi_{++}\left(\frac{1}{x}\right) = \frac{2}{3+\varepsilon}\varphi_{+,-\varepsilon}(x); \tag{31}$$

$$\varphi_{+-}(1-x) = 2\chi(2)\varphi_{-+}(x),\quad x^{n+-}\varphi_{+-}\left(\frac{1}{x}\right) = \frac{4}{3-\varepsilon}\varphi_{+,\varepsilon}(x); \tag{32}$$

$$\varphi_{-+}(1-x) = \frac{1}{2}\chi(2)\varphi_{+-}(x),\quad x^{n-+}\varphi_{-+}\left(\frac{1}{x}\right) = \frac{2}{-1+3\varepsilon}\varphi_{-,\varepsilon}(x); \tag{33}$$

$$\varphi_{--}(1-x) = -\chi(2)\varphi_{--}(x),\quad x^{n--}\varphi_{--}\left(\frac{1}{x}\right) = \frac{4}{1+3\varepsilon}\varphi_{-,-\varepsilon}(x) \tag{34}$$

angegeben.[12])

Satz 8. *Definiert man die Polynome $A(x)$, $B(x)$ in P durch*

$$[(1+z)(1+z^p)(1+z^{p^2})\ldots(1+z^{p^{n-1}})]^{\frac{p-1}{2}} = A(z^2) + zB(z^2), \tag{35}$$

so gilt

$$\varphi_{++}(x) = A(x) + xB(x), \tag{36}$$

$$\varphi_{+-}(x) = 2[A(x) + B(x)], \tag{37}$$

$$\varphi_{-+}(x) = A(x), \tag{38}$$

$$\varphi_{--}(x) = -2B(x).^{13}) \tag{39}$$

---

[11]) Insbesondere für $n=1$ entsprechen den vier Paaren ϱ, σ in der Theorie der Verteilung der quadratischen Reste die vier Arten sogenannter zweigliedriger Sequenzen. [Man schreibe die zweite Gleichung (30) in der Form $\chi(a-1) = -\varepsilon\sigma$.] Somit enthält (15) den Satz von LAGRANGE über die Anzahl dieser Sequenzen als Nebenresultat. — Nach den bisherigen beherrscht man die zweigliedrigen Sequenzen durch die obigen hypergeometrischen Reihen. Ähnliches erwartet man für die dreigliedrigen Sequenzen nicht mehr [hierzu müßte man die acht größten gemeinschaftlichen Teiler

$$\left(1 \pm x^{\frac{p-1}{2}},\ 1 \pm (1+x)^{\frac{p-1}{2}},\ 1 \pm (2+x)^{\frac{p-1}{2}}\right)$$

bestimmen], da deren Theorie unvergleichbar schwieriger ist. Merkwürdigerweise treten schon bei der Bestimmung der Anzahl der dreigliedrigen Sequenzen wieder hypergeometrische Reihen auf, die aber keine algebraischen Funktionen sind. An einer anderen Stelle möchte ich hierauf zurückkommen.

[12]) Es ist $\chi(2) = 1$ für $q \equiv \pm 1 \pmod 8$ und $\chi(2) = -1$ für $q \equiv \pm 3 \pmod 8$. — Nach (31)—(34) bewirken die Substitutionen $x \to 1-x$, $x \to \frac{1}{x}$ im wesentlichen eine Permutation der $\varphi_{\varrho\sigma}(x)$, die auch von (30) abzulesen ist.

[13]) Im Satz 8 ist weiter nichts neues geschehen, als daß wir die im Satz 4 genannten Partialsummen von $F_{\varrho\sigma}(x)$ [im Körper P] berechnet haben; das sind die

Satz 9. *Die Faktorenzerlegung* (29) *von* $1-x^{q-1}$ *läßt sich ein wenig verfeinern, und zwar zerfällt* $\varphi_{--}(x)$ *im Fall* $q\equiv 1 \pmod 4$ *in zwei Faktoren, die die Partialsummen der hypergeometrischen Reihen*

$$(40)\qquad \frac{1}{2}\left[(1+\sqrt{x})^{-\frac{1}{4}}+(1-\sqrt{x})^{-\frac{1}{4}}\right]=1+\sum\binom{-\frac{1}{4}}{2k}x^k,$$

$$(41)\qquad -\frac{2}{\sqrt{x}}\left[(1+\sqrt{x})^{-\frac{1}{4}}-(1-\sqrt{x})^{-\frac{1}{4}}\right]=1-4\sum\binom{-\frac{1}{4}}{2k+1}x^k$$

vom Grad $\mathcal{E}\left(\frac{q-1}{8}\right)$[14]) *bzw.* $\mathcal{E}\left(\frac{q-5}{8}\right)$ *sind, und* $\varphi_{+-}(x)$ *zerfällt im Fall* $q\equiv -1 \pmod 4$ *ebenfalls in zwei Faktoren, die die Partialsummen von*

$$(42)\qquad \frac{1}{2}\left[(1+\sqrt{x})^{\frac{1}{4}}+(1-\sqrt{x})^{\frac{1}{4}}\right]=1+\sum\binom{\frac{1}{4}}{2k}x^k,$$

$$(43)\qquad \frac{2}{\sqrt{x}}\left[(1+\sqrt{x})^{\frac{1}{4}}-(1-\sqrt{x})^{\frac{1}{4}}\right]=1+4\sum\binom{\frac{1}{4}}{2k+1}x^k$$

vom Grad $\mathcal{E}\left(\frac{q+1}{8}\right)$ *bzw.* $\mathcal{E}\left(\frac{q-3}{8}\right)$ *sind.*[15])

Satz 10. *Es sind im Fall* $q\equiv\pm 1 \pmod 8$

$$(44)\qquad \frac{1}{2}[1+\varphi_{++}(x)],\quad \frac{8}{x(1-x)}[1-\varphi_{++}(x)],$$

im Fall $q\equiv\pm 3 \pmod 8$ *aber*

$$(45)\qquad \frac{1}{2(1-x)}[1+\varphi_{++}(x)],\quad \frac{8}{x}[1-\varphi_{++}(x)]$$

---

(36)–(39). — Der Grad der linken Seite von (35) ist $\frac{1}{2}(p^n-1)$, die Anzahl der Entwicklungsglieder bloß $\left(\frac{p+1}{2}\right)^n$ [diese sind aber auch schon alle $\neq 0$ in P]. Hiermit ist dieses Polynom für $n\geqq 2$ lückenhaft und die Lückenhaftigkeit steigert sich für wachsendes n stark. Dies überträgt sich kraft (35) auf $A(x)$ und $B(x)$, und dann weiter nach (36)—(39) auf die $\varphi_{\varrho\sigma}(x)$. [Für die Reihen (24)–(27) folgt aus Satz 4, daß die natürliche Dichte der mod p nichtverschwindenden Koeffizienten Null ist.]

[14]) Für reelles x bedeutet $\mathcal{E}(x)$ die größte ganze Zahl $\leqq x$.

[15]) Folglicherweise zerfallen auch die hier angegebenen Polynome in Q in lauter verschiedene Linearfaktoren. Es ist uns nicht gelungen die Nullstellen dieser Polynome näher zu bestimmen. Obige hypergeometrische Reihen sind die Fälle $v=\pm\frac{1}{4}$ von (17), (18).

(ganze) normierte Quadratpolynome in P. In beiden Fällen ist das Produkt der genannten zwei Polynome gleich $\varphi_{--}^2(x)$.[16])

Satz 11. *Es ist*

$$f(x) = \frac{1 + \frac{x}{2}\varphi_{+-}(x^2)}{1 + \chi(2)\,x} \tag{46}$$

ein (ganzes) normiertes Quadratpolynom in P. Zugleich gilt

$$f(x)f(-x) = \varphi_{-+}^2(x^2).^{17}) \tag{47}$$

Satz 12. *Für* $p \geqq 5$ *sind*

$$\frac{1}{2}\left[1 + 3x + (3x^2 + x^3)\,x^{\frac{q-3}{2}} + (1-x)^{\frac{q+3}{2}}\right], \tag{48}$$

$$\frac{2}{9x}\left[1 + 3x + (3x^2 + x^3)\,x^{\frac{q-3}{2}} - (1-x)^{\frac{q+3}{2}}\right], \tag{49}$$

$$\frac{1}{2(1-x)^3}\left[1 + 3x - (3x^2 + x^3)\,x^{\frac{q-3}{2}} + (1-x)^{\frac{q+3}{2}}\right], \tag{50}$$

$$\frac{2}{9x(1-x)^3}\left[1 + 3x - (3x^2 + x^3)\,x^{\frac{q-3}{2}} - (1-x)^{\frac{q+3}{2}}\right] \tag{51}$$

(ganze) normierte Quadratpolynome in P.[18])

Beweis.[19]) Für jedes x in Q ist

$$\chi(x) = x^{\frac{q-1}{2}}; \tag{52}$$

diese Gleichung ist so zu verstehen, daß man den Wert 0, 1 bzw. -1 der linken Seite in Q deutet. Nach diesem ist für jedes x in Q

---

[16]) Die Quadratwurzeln der Polynome (44), (45) liefern also eine Faktorenzerlegung von $\varphi_{--}(x)$, die von der im Satz 9 für den Fall $q \equiv 1 \pmod 4$ angegebenen verschieden ist. Diese Quadratwurzeln und die Nullstellen konnten wir aber nicht näher bestimmen.

[17]) Man sieht, daß $f(x)$ in Q in lauter zweifache Linearfaktoren zerfällt, auch die Nullstellen sind bis auf das Vorzeichen leicht anzugeben. Die Quadratwurzel von $f(x)$ konnten wir wieder nicht bestimmen.

[18]) Abweichend von den bisherigen Sätzen handelt es sich im Satz 12 nicht mehr um die $\varphi_{\varrho\sigma}(x)$. — Es wäre leicht zu beweisen, daß die Quadratwurzeln aus (48)—(51) wieder Partialsummen von (17) und (18) für $\nu = \frac{3}{2}$ und $\nu = -\frac{3}{2}$ sind. Satz 12 würde sich leicht verallgemeinern lassen entsprechend den Fällen $\nu = \pm\frac{5}{2}, \pm\frac{7}{2}, \ldots$ Da wir in Satz 12 weniger Interesse erblicken als in den vorangehenden, wollten wir ihn und werden auch seinen Beweis möglichst kurz fassen.

[19]) Den etwas mühsamen Beweis der Sätze 4, 8, 9 lassen wir erst am Ende folgen, nehmen aber Satz 4 beim Beweis der Sätze 7, 10, 11 vorweg.

$$\Phi_{++}(x)=\frac{1}{2}[1+\chi(x)\,x+\chi(1-x)\,(1-x)],$$

und für die übrigen $\Phi_{\varrho\sigma}(x)$ gilt ähnliches. Hieraus folgt Satz 1 leicht.

Man sieht, daß einerseits die $\varphi_{\varrho\sigma}(x)$ andererseits die $\Phi_{\varrho\sigma}(x)$ paarweise teilerfremd sind, und daß $\varphi_{\varrho\sigma}(x)\,|\,\Phi_{\varrho\sigma}(x)$ ist. Weiter ist dann nach (12):

$$\varphi_{+,\sigma}(x)\,\varphi_{-,\sigma}(x)=(1-x^{q-1},\ 1+\sigma(1-x)^{\frac{q-1}{2}}),$$

$$\text{(53)}\qquad \prod_{\varrho,\,\sigma=\pm 1}\varphi_{\varrho\sigma}(x)=(1-x^{q-1},\ 1-(1-x)^{q-1})=\frac{1-x^{q-1}}{1-x},$$

da

$$1-(1-x)^{q-1}=1-\frac{(1-x)^q}{1-x}=1-\frac{1-x^q}{1-x}=-x\frac{1-x^{q-1}}{1-x}$$

ist. Ähnlich aber noch leichter berechnet man aus (3)—(6):

$$\prod_{\varrho,\,\sigma=\pm 1}\Phi_{\varrho\sigma}(x)=\left(\frac{1-x^{q-1}}{1-x}\right)^2.$$

Vergleicht man dies mit (53), so entsteht nach obigen Bemerkungen (14), d. h. auch Satz 2.

Von (3)—(6) liest man leicht ab, daß der Grad der Reihe nach das doppelte der Zahlen (15) ist. Hieraus und aus (14) folgt Satz 3.

Im Satz 5 ist (29) nichts anderes als (53). Aus (29) folgen aber auch die Gleichungen (28), da in diesen nach (8)—(11) die linke Seite durch die Faktoren der rechten Seite teilbar ist. Also ist Satz 5 richtig.

Nach (52) ist klar, daß jedes a in (30) eine Nullstelle von $\varphi_{\varrho\sigma}(x)$ ist. Andererseits erschöpfen die zu allen Paaren ϱ, σ gehörenden a die Elemente $\neq 0, 1$ von Q, deren Anzahl $q-2$ gleich der Summe der Grade der $\varphi_{\varrho\sigma}(x)$ ist. Hieraus folgt Satz 6.

Um Satz 7 zu beweisen zeigen wir zuerst:

$$\text{(54)}\qquad \varphi_{++}(x)=1+\ldots+\frac{2}{3+\varepsilon}\,x^{n++},$$

$$\text{(55)}\qquad \varphi_{+-}(x)=1+\ldots+\frac{4}{3-\varepsilon}\,x^{n+-},$$

$$\text{(56)}\qquad \varphi_{-+}(x)=1+\ldots+\frac{2}{-1+3\varepsilon}\,x^{n-+},$$

$$\text{(57)}\qquad \varphi_{--}(x)=1+\ldots+\frac{4}{1+3\varepsilon}\,x^{n--}.$$

Ursprünglich wären nämlich die letzten Koeffizienten nach Satz 4 [19])

und (15):

$$\binom{\frac{1}{2}}{\frac{q-\varepsilon}{2}},\ 2\binom{\frac{1}{2}}{\frac{q+\varepsilon}{2}},\ \binom{-\frac{1}{2}}{\frac{q-2+\varepsilon}{2}},\ -2\binom{-\frac{1}{2}}{\frac{q-2-\varepsilon}{2}}.$$

In den Binomialkoeffizienten läßt sich der Zähler $\pm\frac{1}{2}$ durch $\frac{q\pm 1}{2}$ ersetzen, und dann gehen sie durch die Umformung $\binom{u}{v}=\binom{u}{u-v}$ in

$$\binom{\frac{q+1}{2}}{\frac{1+\varepsilon}{2}}=\frac{2}{3+\varepsilon},\ \binom{\frac{q+1}{2}}{\frac{1-\varepsilon}{2}}=\frac{2}{3-\varepsilon},\ \binom{\frac{q-1}{2}}{\frac{1-\varepsilon}{2}}=\frac{2}{-1+3\varepsilon},\ \binom{\frac{q-1}{2}}{\frac{1+\varepsilon}{2}}=\frac{-2}{1+3\varepsilon}$$

über, wodurch (54)—(57) bewiesen ist.

Aus (30) folgt, daß einerseits

(58) $$\varphi_{\varrho\sigma}(1-x) \text{ und } \varphi_{\sigma\varrho}(x)$$

andererseits wegen

$$\chi\left(\frac{1}{a}\right)=-\varrho,\quad \chi\left(1-\frac{1}{a}\right)=\varepsilon\varrho\sigma$$

auch

(59) $$x^{n\varrho\sigma}\varphi_{\varrho\sigma}\left(\frac{1}{x}\right) \text{ und } \varphi_{\varrho,-\varepsilon\varrho\sigma}(x)$$

assoziiert sind. Die Polynompaare in (58), (59) sind eben die in den Gleichungen (31)—(34) von den rechtsseitigen konstanten Faktoren abgesehen. Weiter liest man von (54)—(57) leicht ab, daß unter den Gleichungen (31)—(34) in den vorderen die Koeffizienten der Glieder höchsten Grades, in den hinteren aber die konstanten Glieder gleich sind. Dabei (beim ersteren) ist nämlich zu berücksichtigen, daß nach (15)

$$(-1)^{n++}=\chi(2),\ (-1)^{n+-}=(-1)^{n-+}=\varepsilon\chi(2),\ (-1)^{n--}=-\chi(2)$$

ist. Damit haben wir Satz 7 bewiesen.

Für Satz 10 beweisen wir zuerst, daß (44), (45) ganze Polynome sind. Diese Behauptung ist gleichwertig mit $\varphi_{++}(0)=1$, $\varphi_{++}(1)=\chi(2)$ [vgl.[12]]. Die erste Gleichung sagt nichts anderes, als daß $\varphi_{++}(x)$ normiert ist; die zweite folgt dann aus der ersten Gleichung in (31).

Weiter gewinnen wir aus (3) und (6):

$$4\Phi_{++}(x)+x(1-x)\,\Phi_{--}(x)=4$$

d. h. nach (14)

$$4[1+\varphi_{++}(x)][1-\varphi_{++}(x)]=x(1-x)\,\varphi^2_{--}(x).$$

Man sieht hieraus, daß das Produkt der Polynome (44) bzw. (45) in der Tat $\varphi^2_{--}(x)$ ist. Da beidesmal die Faktoren teilerfremd sind, so sind

sie auch Quadratpolynome. Endlich sind sie auch normiert, da dies für die vorderen Polynome in (44), (45) klar ist und das gleiche auch für $\varphi_{--}(x)$ gilt. Damit haben wir Satz 10 bewiesen.

Zu Satz 11 zeigen wir zunächst, daß $f(x)$ in (46) ein ganzes Polynom ist. Da der lineare Nenner die Nullstelle $x=-\chi(2)$ hat, so ist nur zu zeigen, daß für dieses x auch der Zähler verschwindet, d. h. $1-\frac{1}{2}\chi(2)\varphi_{+-}(1)=0$ ist. Letzteres folgt in der Tat aus $\varphi_{-+}(0)=1$ und der ersten Gleichung in (32).

Da nach (46) $f(x)$ normiert ist und $f(x)$, $f(-x)$ offenbar teilerfremd sind, brauchen wir nur noch (47) zu beweisen, woraus dann nämlich folgt, daß die Faktoren links Quadratpolynome sind. Nach (46) und (14) ist

$$f(x)f(-x)=\frac{1-\frac{x^2}{4}\Phi_{+-}(x^2)}{1-x^2}.$$

Andererseits folgt aus (4) und (5):

$$x\Phi_{+-}(x)+4(1-x)\Phi_{-+}(x)=4.$$

Aus beiden entsteht $f(x)f(-x)=\Phi_{-+}(x^2)$, d. h. wegen (14) auch (47). Also ist Satz 11 richtig.

Satz 12 ergibt sich so. Man prüft leicht nach, daß die Polynome (48)—(51) ganz und normiert sind. Dann bezeichne man diese Polynome der Reihe nach mit $\Psi_{++}(x)$, $\Psi_{+-}(x)$, $\Psi_{-+}(x)$, $\Psi_{--}(x)$. Offenbar ist

$$\Psi_{\varrho,+}(x)\Psi_{\varrho,-}(x)= \tag{60}$$
$$=\frac{1}{9x}(1-x)^{3(\varrho-1)}\left[(1+3x+\varrho(3+x)x^{\frac{\varrho+1}{2}})^2-(1-x)^{\varrho+3}\right].$$

Wegen $(1-x)^q=1-x^q$ berechnet sich der Ausdruck in [] leicht zu

$$x(3+x+\varrho(1+3x)x^{\frac{\varrho-1}{2}})^2.$$

Da hiernach die rechte Seite von (60) ein Polynomquadrat ist und nach (48), (49) bzw. (50), (51) die Faktoren der linken Seite teilerfremd sind, so sind sie nach obigem auch Polynomquadrate. Das beweist Satz 12.

Als Vorbereitung zum Beweis der Sätze 4, 8, 9 zeigen wir zuerst folgendes:

Ist a eine rationale für p ganze Zahl mit der p-adischen Entwicklung

$$a=a_0+a_1p+a_2p^2+\ldots \qquad (0\leqq a_i\leqq p-1;\ i=0,1,\ldots), \tag{61}$$

so ist

$$(1+x)^a=1+\sum\binom{a}{k}x^k=(1+x)^{a_0}(1+x^p)^{a_1}(1+x^{p^2})^{a_2}\ldots, \tag{62}$$

wobei das zweite „=“ in P zu deuten ist so nämlich, daß nach Ausmultiplizieren die entsprechenden Koeffizienten in P gleich sind. Mit anderen Worten, indem wir noch

$$k = k_0 + k_1 p + \ldots + k_e p^e \qquad (0 \leqq k_i \leqq p-1\,;\ i = 0, 1, \ldots, e) \tag{63}$$

setzen, gilt in P:

$$\binom{a}{k} = \binom{a_0}{k_0}\binom{a_1}{k_1} \ldots \binom{a_e}{k_e}. \tag{64}$$

Betrachten wir nämlich die Partialsumme

$$S_l = 1 + \sum_{k=1}^{p^{l+1}-1} \binom{a}{k} x^k \qquad (l = 0, 1, \ldots) \tag{65}$$

der Potenzreihe in (62). Da nach (61)

$$a \equiv a_0 + a_1 p + \ldots + a_l p^l \pmod{p^{l+1}}$$

ist, gilt in P offenbar

$$S_l = 1 + \sum \binom{a_0 + a_1 p + \ldots + a_l p^l}{k} x^k, \tag{66}$$

wobei rechts nur formal eine unendliche Reihe steht, da die Koeffizienten für $k \geqq p^{l+1}$ sicher verschwinden. Es ist (66) nichts anderes als

$$S_l = (1+x)^{a_0 + a_1 p + \ldots + a_l p^l}.$$

Nun gilt in P die Regel $(u+v)^p = u^p + v^p$, woraus weiter folgt:

$$S_l = (1+x)^{a_0}(1+x^p)^{a_1} \ldots (1+x^{p^l})^{a_l}.$$

Da l beliebig groß sein darf, ist (62) richtig, womit die Behauptung bewiesen ist.

Jetzt beweisen wir Satz 4. Es gilt p-adisch

$$\pm\frac{1}{2} = \frac{p \pm 1}{2} + \frac{p-1}{2} p + \frac{p-1}{2} p^2 + \ldots, \tag{67}$$

woraus nach (64) folgt:

$$\binom{\pm\frac{1}{2}}{k} = \binom{\frac{p \pm 1}{2}}{k_0}\binom{\frac{p-1}{2}}{k_1} \ldots \binom{\frac{p-1}{2}}{k_e}. \tag{68}$$

Man bemerke gleich, daß dies in P verschwindet, wenn $\frac{1}{2}(p^{e+1} \pm 1) < k < p^{e+1}$ ist, da dann wegen

$$\frac{p \pm 1}{2} + \frac{p-1}{2} p + \ldots + \frac{p-1}{2} p^e = \frac{1}{2}(p^{e+1} \pm 1)$$

wenigstens ein k_i größer ist als die darüber stehende Zahl.

Betrachten wir in P die vier Koeffizientenfolgen in (24)—(27):

$$\binom{\frac{1}{2}}{2k}; \quad \binom{\frac{1}{2}}{2k+1}; \quad \binom{-\frac{1}{2}}{2k}; \quad \binom{-\frac{1}{2}}{2k+1} \qquad (k = 1, 2, \ldots). \tag{69}$$

Die Glieder bzw. mit den Stellenzeigern

$$k = \frac{q+1}{2}, \frac{q-1}{2}, \frac{q+1}{2}, \frac{q-1}{2}$$

sind

$$\binom{\frac{1}{2}}{q+1}, \binom{\frac{1}{2}}{q}, \binom{-\frac{1}{2}}{q+1}, \binom{-\frac{1}{2}}{q}$$

d. h. nach (68):

$$-\frac{1}{4}, -\frac{1}{2}, \frac{1}{4}, -\frac{1}{2}. \tag{70}$$ [20])

Weiter betrachten wir auch die vier Partialfolgen von (69) bestehend aus den Gliedern, die jedesmal den eben geprüften Gliedern voranstehen (d. h. in denen $2k$ bzw. $2k+1 < q$ ist). In diesen endlichen Folgen verschwinden (in P) die Glieder bzw. mit $k >$

$$\mathscr{E}\left(\frac{q+1}{4}\right), \mathscr{E}\left(\frac{q-1}{4}\right), \mathscr{E}\left(\frac{q-1}{4}\right), \mathscr{E}\left(\frac{q-3}{4}\right), \tag{71}$$

wie man das aus der Bemerkung bei (68) leicht sieht. Nach (15) ist aber (71) eben n_{++}, n_{+-}, n_{-+}, n_{--}.

All dies ergibt nach (24)—(27) in P (vgl.[20])):

$$F_{\varrho\sigma}(x) = \{F_{\varrho\sigma}(x)\} - \varrho 2^{-1-\sigma} x^{\frac{q+\sigma}{2}} + \ldots \qquad (\varrho, \sigma = \pm 1), \tag{72}$$

wobei $\{F_{\varrho\sigma}(x)\}$ die Partialsumme vom Grad $n_{\varrho\sigma}$ von $F_{\varrho\sigma}(x)$ ist. Da nach (15') $2n_{\varrho\sigma} \leqq \frac{q+\sigma}{2}$ ist, folgt aus (72) nach Quadrieren

$$F^2_{\varrho\sigma}(x) = \{F_{\varrho\sigma}(x)\}^2 - \varrho 2^{-\sigma} x^{\frac{q+\sigma}{2}} + \ldots,^{21}) \tag{73}$$

wobei berücksichtigt werden mußte, daß $\{F_{\varrho\sigma}(x)\}$ das Anfangsglied 1 hat.

Andererseits ergibt (23):

$$2^{\sigma} x^{\frac{1-\sigma}{2}} (1-x)^{\frac{1-\varrho}{2}} F^2_{\varrho\sigma}(x) = 1 + \sigma(1-x)^{\frac{1}{2}}. \tag{74}$$

Außerdem gilt in P offenbar

$$(1-x)^{\frac{1}{2}} = (1-x)^{\frac{q+1}{2}} + \ldots,^{22}) \tag{75}$$

wobei links die Potenzreihe zu nehmen ist.

---

[20]) Das entsprechende Glied von $F_{\varrho\sigma}(x)$ in (24)—(27) ist dann bzw. $-\frac{1}{4} x^{\frac{q+1}{2}}$, $-x^{\frac{q-1}{2}}$, $\frac{1}{4} x^{\frac{q+1}{2}}$, $x^{\frac{q-1}{2}}$ d. h. allgemein für alle vier Fälle: $-\varrho 2^{-1-\sigma} x^{\frac{q+\sigma}{2}}$.

[21]) Dies ist natürlich so zu lesen, daß die rechts nicht angeschriebenen Glieder von größerem Grade als $\frac{q+\sigma}{2}$ sind.

[22]) Wieder fehlen rechts nur Glieder vom Grad $> \frac{q+1}{2}$.

Wir setzen (73), (75) in (74) ein:

$$2^{\sigma}x^{\frac{1-\sigma}{2}}(1-x)^{\frac{1-\varrho}{2}}\{F_{\varrho\sigma}(x)\}^2-\varrho x^{\frac{q+1}{2}}(1-x)^{\frac{1-\varrho}{2}}+\ldots=1+\sigma(1-x)^{\frac{q+1}{2}}+\ldots,$$

und berücksichtigen beiderseits nur die Glieder vom Grad $\leqq\frac{q+1}{2}$. Da nach (15') der Grad $\frac{1-\varrho}{2}+\frac{1-\sigma}{2}+2n_{\varrho\sigma}$ des ersten Produkts links $\leqq\frac{q+1}{2}$ ist, entsteht

$$2^{\sigma}x^{\frac{1-\sigma}{2}}(1-x)^{\frac{1-\varrho}{2}}\{F_{\varrho\sigma}(x)\}^2-\varrho x^{\frac{q+1}{2}}=1+\sigma(1-x)^{\frac{q+1}{2}}.$$

Dies mit (7) verglichen ergibt

$$\{F_{\varrho\sigma}(x)\}^2=\Phi_{\varrho\sigma}(x),$$

womit nach (14) Satz 4 bewiesen ist.

Satz 8 folgt so. Aus (62) und (67) ergibt sich in P

$$(1+x)^{-\frac{1}{2}}=[(1+x)(1+x^p)(1+x^{p^2})\ldots]^{\frac{p-1}{2}}$$

und weiter hieraus nach (35) offenbar

$$(76)\qquad (1+x)^{-\frac{1}{2}}=A(x^2)+xB(x^2)+\ldots\ ^{23})$$

Da $A(x)$, $B(x)$ ebenfalls nach (35) bzw. vom Grade

$$(77)\qquad \mathcal{E}\left(\frac{q-1}{4}\right),\ \mathcal{E}\left(\frac{q-3}{4}\right)$$

sind, entsteht nach Multiplikation mit $1+x$ (vgl. [23])) auch noch

$$(78)\qquad (1+x)^{\frac{1}{2}}=(1+x)A(x^2)+(x+x^2)B(x^2)+\ldots$$

Wendet man (78) und (76) mit $\pm\sqrt{x}$ statt x an, so folgt aus (19)–(22):

$$F_{++}(x)=A(x)+xB(x)+\ldots,$$
$$F_{+-}(x)=2[A(x)+B(x)]+\ldots,$$
$$F_{-+}(x)=A(x)+\ldots,$$
$$F_{--}(x)=-2B(x)+\ldots$$

Die Grade der rechts angeschriebenen Polynome sind nach (77) die Zahlen (71) d. h., wie schon bemerkt, eben die n_{++}, $n_{+-},\ldots$ Diese Polynome sind also der Reihe nach die vier $\{F_{\varrho\sigma}(x)\}$, und somit folgt Satz 8 aus Satz 4.

Es ist nur noch übrig Satz 9 zu beweisen. Hierzu bezeichnen wir die Potenzreihen (40)—(43) mit $G_i(x)\,[i=1,\ldots,4]$. Wir betrachten

---

[23]) Die rechts fehlenden Glieder sind von höherem Grade als das Polynom auf der rechten Seite, sie sind sogar vom Grad $\geqq p^n\,(=q)$.

zuerst den Fall $q \equiv 1 \pmod 4$ und zeigen, daß dann in P

$$G_1(x) = \{1 + \ldots + d\, x^{\mathscr{E}\left(\frac{q-1}{8}\right)}\} + e x^{\frac{q+1}{2}} + \ldots, \tag{79}$$

$$G_2(x) = \{1 + \ldots + d' x^{\mathscr{E}\left(\frac{q-5}{8}\right)}\} + e' x^{\frac{q-1}{2}} + \ldots \tag{80}$$

ist, wobei $d, e, \ldots$ irgendwelche Konstanten sind.

Jetzt ist nämlich entweder $p \equiv 1 \pmod 4$ oder $p \equiv -1 \pmod 4$, $2 | n$. Entsprechend gilt p-adisch

$$-\frac{1}{4} = \frac{p-1}{4}(1 + p + p^2 + \ldots),$$

$$-\frac{1}{4} = \left(\frac{3p-1}{4} + \frac{p-3}{4} p\right)(1 + p^2 + p^4 + \ldots),$$

woraus nach (64) in P bzw.

$$\left(\frac{-\frac{1}{4}}{k}\right) = \left(\frac{\frac{p-1}{4}}{k_0}\right)\left(\frac{\frac{p-1}{4}}{k_1}\right)\ldots,$$

$$\left(\frac{-\frac{1}{4}}{k}\right) = \left(\frac{\frac{3p-1}{4}}{k_0}\right)\left(\frac{\frac{p-3}{4}}{k_1}\right)\left(\frac{\frac{3p-1}{4}}{k_2}\right)\ldots$$

folgt. Also hat das letzte in P nichtverschwindende Glied der Folge

$$\left(\frac{-\frac{1}{4}}{1}\right), \ldots, \left(\frac{-\frac{1}{4}}{q-1}\right)$$

den Stellenzeiger

$$k = \frac{p-1}{4} + \frac{p-1}{4} p + \ldots + \frac{p-1}{4} p^{n-1}$$

bzw.

$$k = \left(\frac{3p-1}{4} + \frac{p-3}{4} p\right) + \ldots + \left(\frac{3p-1}{4} p^{n-2} + \frac{p-3}{4} p^{n-1}\right).$$

Da dies beidesmal $\frac{q-1}{4}$ ist, folgen (79), (80) leicht aus (40), (41).

Andererseits ist nach (40), (41), (22)

$$G_1(x)\, G_2(x) = F_{--}(x),$$

woraus nach (79), (80) mit Rücksicht auf (72) und Satz 4 leicht folgt, daß Satz 9 im jetzt betrachteten Fall richtig ist.

Im anderen Fall $q \equiv -1 \pmod 4$ ist $p \equiv -1 \pmod 4$, $2 \nmid n$. Es gilt p-adisch

$$\frac{1}{4} = \frac{p+1}{4} + \left(\frac{3p-1}{4} + \frac{p-3}{4} p\right)(p + p^3 + p^5 + \ldots).$$

Dies ergibt nach (64) ähnlich wie früher, daß in der Folge

$$\binom{\frac{1}{4}}{1},\ldots,\binom{\frac{1}{4}}{q-1}$$

der Stellenzeiger des letzten in P nichtverschwindenden Gliedes

$$k=\frac{p+1}{4}+\left(\frac{3p-1}{4}p+\frac{p-3}{4}p^2\right)+\ldots+$$
$$+\left(\frac{3p-1}{4}p^{n-2}+\frac{p-3}{4}p^{n-1}\right)=\frac{q+1}{4}$$

ist. Hieraus und aus (42), (43) folgen

$$G_3(x)=\{1+\ldots+d''\,x^{\mathcal{E}\left(\frac{q+1}{8}\right)}\}+e''\,x^{\frac{q+1}{2}}+\ldots,$$
$$G_4(x)=\{1+\ldots+d'''x^{\mathcal{E}\left(\frac{q-3}{8}\right)}\}+e'''x^{\frac{q-1}{2}}+\ldots,$$

wobei d'', e'', ... irgendwelche Konstanten sind.

Andererseits ist nach (42), (43), (20)

$$G_3(x)\,G_4(x)=F_{+-}(x).$$

Man gewinnt ähnlich wie vorher, daß Satz 9 auch im vorliegenden Fall richtig ist.

Bemerkung. Es ist auffällig, wie viele Polynome mit sehr einfachen Koeffizienten in P sich finden ließen, aus denen man die Quadratwurzel ausziehen kann (Sätze 2, 10, 11, 12). Wir wollen die interessante Folgerung noch besonders hervorheben, daß für das Polynom $\Phi_{++}(x)$ in (3) nach den Sätzen 2 und 10 gilt: Es sind

$$\sqrt{2(1+\sqrt{\Phi_{++}(x)})},\quad \sqrt{\frac{2(1-\sqrt{\Phi_{++}(x)})}{x(1-x)}}\quad [q\equiv\pm 1 \pmod 8]$$

bzw.

$$\sqrt{\frac{2(1+\sqrt{\Phi_{++}(x)})}{1-x}},\ \sqrt{\frac{2(1-\sqrt{\Phi_{++}(x)})}{x}}\quad [q\equiv\pm 3 \pmod 8]$$

rationale Polynome in P, wobei das Vorzeichen der inneren Quadratwurzel so gewählt wird, daß $\sqrt{\Phi_{++}(x)}=1+\ldots$ ist. — Es wäre leicht die Potenzsummen der a in (30) zu bestimmen. Wollte man aber hieraus mit Hilfe der Newtonschen Formeln die elementarsymmetrischen Funktionen der a, also die Polynome $\varphi_{\varrho\sigma}(x)$ bestimmen, so wäre das ein viel komplizierterer Weg. (Das war unser Verfahren in der Arbeit[4]).)

(Eingegangen am 2. Mai 1944).